06-19943 Jan. 28, 1994 L6: 3 of 4

ELECTRONIC VOTING SYSTEM

INVENTOR: ATSUSHI FUJIOKA, et al. (1)
ASSIGNEE: NIPPON TELEGR & TELEPH CORP <NTT>, et al. (20)
APPL NO: 04-170899
DATE FILED: Jun. 29, 1992
PATENT ABSTRACTS OF JAPAN
ABS GRP NO: P1731
ABS VOL NO: Vol. 18, No. 232
ABS PUB DATE: Apr. 27, 1994
INT-CL: G06F 15/28; G07C 13/00

ABSTRACT:

PURPOSE:To obtain a safe and fair electronic voting method capable of holding privacy by ciphering the contents of a vote to form a voting sentence and transmitting a disturbed voting sheet with a signature to an election supervisor.

CONSTITUTION:Respective voter devices 100 for T voters Vi are connected to an election supervisor device 200 through a register communication line 400 and connected also to a totalizer device 300 through an anonymous communication line 500. The device 300 opens a table 600 for the contents of votes. The device 100 is constituted so as to access the table 600. Since a voting sentence disturbed the contents of a vote by a random number, an election supervisor A and a totalizer C can not find out the contents of the vote from the disturbed voting sentence and unsigned voting is also guaranteed. Since a formal objection claiming a valid voter Vi is shown only by transmitting the ciphered voting sentence and the signature of the supervisor A to the totalizer C, it can be executed without clarifying the contents of the vote.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開平6－19943
(43)公開日　平成６年(1994)１月28日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　15/28		Ｂ　7052－5Ｌ		
Ｇ０７Ｃ　13/00		Ｂ　9146－3Ｅ		

審査請求　未請求　請求項の数２(全　９　頁)

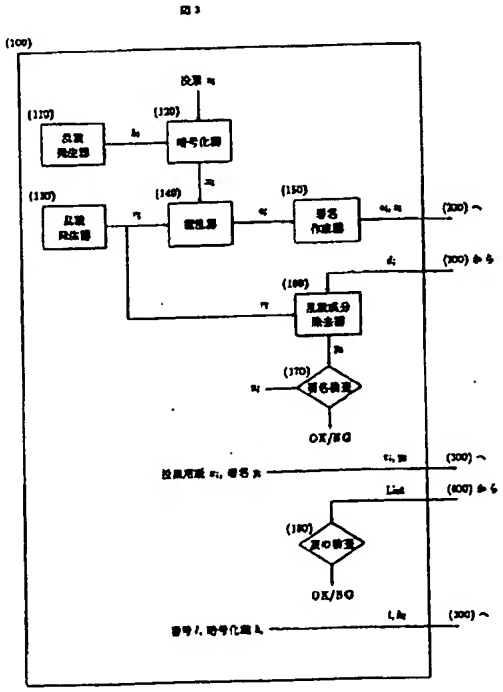
(21)出願番号　特願平4－170899

(22)出願日　平成４年(1992)６月29日

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区内幸町一丁目１番６号
(72)発明者　藤岡　淳
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内
(72)発明者　岡本　龍明
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内
(74)代理人　弁理士　草野　卓

(54)【発明の名称】　電子投票方法および装置

(57)【要約】
【目的】　匿名性を保持し、安全、公平な電子投票方法および装置を提供する。
【構成】　投票者V_iが投票内容v_iを乱数成分k_iにより暗号化し、乱数成分r_iにより撹乱して投票文e_iを作成し、e_iに署名s_iを付してこれを選挙管理者Ａに送信し、選挙管理者Ａは署名s_iに基づいて投票者V_iの正当性を認証した後に、投票文e_iに選挙管理者Ａが署名d_iして署名d_i付き投票文を投票者V_iに返送し、投票者V_iは選挙管理者Ａ署名付き投票文x_i、y_iを求めてこれを集計者Ｃに送信し、集計者Ｃは受信した投票文が選挙管理者Ａによって署名されていることを確認した後に投票文を暗号化されたまま一覧公開し、投票者V_iは自己の投票文が登録されている場合は暗号化に使用した乱数成分k_iを集計者Ｃに送信する一方、登録されていない場合は集計者Ｃに対して異議を申し立て、集計者Ｃは投票内容を集計する電子投票方法および装置。



1

【特許請求の範囲】

【請求項1】　投票者が投票内容を乱数成分により暗号化し、乱数成分により撹乱して投票文を作成し、これに署名を付して選挙管理者に送信し、選挙管理者は付加された署名に基づいて投票者の正当性を認証した後に、投票文に選挙管理者が署名して選挙管理者署名付き投票文を投票者に返送し、投票者は選挙管理者署名付き投票文を求めてこれを集計者に送信し、集計者は受信した投票文が選挙管理者によって署名されていることを確認した後に投票文を暗号化されたまま一覧公開し、投票者は公開された投票文の一覧表に自分の投票文が登録されていることを確認した場合は暗号化に使用した乱数成分を集計者に送信する一方、登録されていない場合は集計者に対して異議を申し立て、集計者は投票文から全ての投票内容を取り出してこれを集計する電子投票方法。

【請求項2】　乱数発生器を使用して生成した乱数成分を入力して投票内容を暗号化する暗号化器、乱数発生器を使用して生成した乱数成分を入力して撹乱された投票文を作成する撹乱器、撹乱器が作成した投票文を入力してこれに署名を付して選挙管理者装置に送信する署名作成器、選挙管理者署名付き投票文を入力してこれから乱数成分の影響を取り除いて暗号化された投票文の署名情報を求める乱数成分除去器、署名情報を確認する署名検査器、暗号化された投票内容および署名情報を集計者装置に送信する装置、自己の投票文が表に存在することを確認したことに基づいて暗号化に使用した乱数成分を集計者装置に送信する装置より成る投票者装置を具備し、投票者確認のなされた撹乱された投票文を入力して選挙管理者署名付き投票文を作成してこれを投票者装置に返送する署名作成器より成る選挙管理者装置を具備し、署名付き投票文をに入力して投票文が選挙管理者装置により署名されていること確認する署名検査器、投票文を表にしてこれを周知せしめる表作成器、投票文を集計する集計器より成る集計者装置を具備する、

ことを特徴とする電子投票装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】この発明は、電子投票方法および装置に関し、特に、電気通信装置を介してアンケート調査その他の投票を実施する場合に、安全で、かつ、公平な無記名投票を実施することができる電子投票方法および装置に関する。

【0002】

【従来の技術】無記名投票は、投票者と投票内容の対応を秘密にすることができ、個人の思想信条に関するプライバシーを守るのに適しているので、電子会議およびCATVの如く双方向電気通信装置を採用している場合のアンケート調査その他の調査、投票に利用することができる。

【0003】双方向電気通信装置において、安全で、かつ、公平な無記名投票を実施するには、投票者の偽装、二重投票、投票文の盗聴に伴う投票内容の漏洩その他の不都合を防止する必要がある。これら不都合を解決する方法としてディジタル署名を採用した電子投票方法が提案されており、これには、例えば、太田和夫：“単一の選挙管理者を用いた電子投票方式”、昭和63年電子情報通信学会春季全国大会、A－294（昭63－3）がある。

2

【0004】

【発明が解決しようとする課題】しかし、この方法には解決されるべき課題が内存している。先ず、選挙管理者が不正を行った場合、投票者がこれに異議申立を行うには投票者の投票内容を公開することが必要であり、これは投票者のプライバシーを侵害する。

【0005】また、選挙管理者には匿名の形で投票が集まるが、その内容は全て選挙管理者には可読であるので、例えば、投票の途中経過を投票者に漏洩することにより選挙結果を左右することが可能である。この発明は、プライバシーを侵害されることなく異議申立をすることができると共に、集計の途中経過が投票に影響を及ぼす余地のない安全、かつ、公平な電子投票方法および装置を提供するものである。

【0006】

【課題を解決するための手段】投票者V_iが投票内容v_iを乱数成分k_iにより暗号化し、乱数成分r_iにより撹乱して投票文e_iを作成し、これに署名s_iを付して選挙管理者Aに送信し、選挙管理者Aは付加された署名s_iに基づいて投票者V_iの正当性を認証した後に、投票文e_iに選挙管理者Aが署名d_iして選挙管理者A署名d_i付き投票文を投票者V_iに返送し、投票者V_iは選挙管理者A署名付き投票文x_i、y_iを求めてこれを集計者Cに送信し、集計者Cは受信した投票文が選挙管理者Aによって署名されていることを確認した後に投票文を暗号化されたまま一覧公開し、投票者V_iは公開された投票文の一覧表に自分の投票文が登録されていることを確認した場合は暗号化に使用した乱数成分k_iを集計者Cに送信する一方、登録されていない場合は集計者Cに対して異議を申し立て、集計者Cは投票文から全ての投票内容を取り出してこれを集計する電子投票方法を構成した。そして、乱数発生器110を使用して生成した乱数成分k_iを入力して投票内容v_iを暗号化する暗号化器120、乱数発生器130を使用して生成した乱数成分r_iを入力して撹乱された投票文e_iを作成する撹乱器140、撹乱器140が作成した投票文e_iを入力してこれに署名s_iを付して選挙管理者装置200に送信する署名作成器150、選挙管理者署名付き投票文を入力してこれから乱数成分の影響を取り除いて暗号化された投票文の署名情報y_iを求める乱数成分除去器160、署名情報y_iを確認する署名検査器170、暗号化された投票内容x_iおよび署名情報y_iを集計者装置

３００に送信する装置、および自己の投票文が表に存在することを確認したことに基づいて暗号化に使用した乱数成分k_iを集計者装置３００に送信する装置より成る投票者装置１００を具備し、投票者確認のなされた撹乱された投票文e_iを入力して選挙管理者署名付き投票文を作成してこれを投票者装置１００に返送する署名作成器２３０より成る選挙管理者装置２００を具備し、署名付き投票文をに入力して投票文が選挙管理者装置２００により署名されていること確認する署名検査器３１０、投票文を表６００にしてこれを周知せしめる表作成器３２０、および投票文を集計する集計器３４０より成る集計者装置３００を具備する、電子投票装置をも構成した。

【０００７】

【実施例】この発明の実施例を図２を参照して説明する。この発明は、先ず、投票者V_iが投票内容v_iを乱数成分k_iにより暗号化する。投票内容を暗号化した上に、更にこれを乱数r_iにより撹乱して投票文e_iを作成する。投票内容を暗号化した上に更に乱数で撹乱した結果e_iに署名s_iを付してこれを選挙管理者Ａに送信する。選挙管理者Ａは付加された署名s_iに基づいて投票者V_iの正当性を認証した後に、投票文e_iに選挙管理者Ａが署名d_iして選挙管理者Ａ署名d_i付き投票文を投票者V_iに返送する。投票者V_iは選挙管理者Ａ署名付き投票文から乱数の影響を取り除いて署名付き投票文x_i、y_iを求め、これを集計者Ｃに送信する。集計者Ｃは受信した投票文が選挙管理者Ａによって署名されていることを確認した後に、投票文を暗号化されたまま一覧公開する。投票者V_iは公開された投票文の一覧表に自分の投票文が登録されていることを確認した場合、暗号化に使用した乱数成分k_iを集計者Ｃに送信する。もし、登録されていない場合は、集計者Ｃに対して異議を申し立てる。集計者Ｃは投票文から全ての投票内容を取り出し、これを集計する。

【０００８】上述の通りであって、投票文は投票内容を乱数により撹乱してあるので、選挙管理者Ａおよび集計者Ｃは撹乱された投票文から投票内容を求めることができず、投票の無記名性も保障される。そして、異議申立に関しても、自分が正当な投票者V_iであることは暗号化されている投票文および選挙管理者Ａの署名を集計者Ｃに対して送信することのみにより示すことができるので、投票内容を明らかにすることなくして異議申立を実施することができる。また、集計者Ｃには暗号化された投票内容が集まるので、投票中にその途中経過は明らかになず、公平な投票方式であると言うことができる。即ち、この発明は従来より指摘されていた異議申立時のプライバシーの侵害および途中経過の漏洩による投票への不正な影響を防止することができるものである。

【０００９】この発明の具体的実施例を図１を参照して説明する。図１（ａ）はこの発明の全体構成を示す図である。図１（ｂ）は投票後の投票内容の一覧を示し、図１（ｃ）は集計後の投票内容の一覧を示す。ここで、Ｔ人の投票者V_iそれぞれの投票者装置１００は、それぞれ記名通信路４００を介して選挙管理者装置２００に接続すると共に、匿名通信路５００を介して集計者装置３００に接続している。集計者装置３００は投票内容の一覧表６００を公開する。投票者装置１００はこの一覧表６００にアクセスすることができる様構成されている。図２はこの発明の通信シーケンスを示し、図３は投票者装置１００を示し、図４は選挙管理者装置２００を示し、図５は集計者装置３００を示す。

【００１０】ここで、これらの図を参照して、投票者V_iが投票内容v_iを選挙管理者Ａの承認を得た後に集計者Ｃに対して投票する場合について説明する。ここで、簡単のために、以下の記法を採用する。

$x=\xi(v,k)$：暗号化関数（メッセージｖ、乱数成分ｋ）

$v=\rho(x,k)$：復号化関数（暗号文ｘ、乱数成分ｋ）

$s=\sigma_i(m)$：投票者V_iの署名作成関数（メッセージｍ）

$m=\zeta_i(s)$：投票者V_iの署名検証関数（署名ｓ）

$s=\sigma_A(m)$：選挙管理者Ａの署名作成関数（メッセージｍ）

$m=\zeta_A(s)$：選挙管理者Ａの署名検証関数（署名ｓ）

$e=\omega_A(m,r)$：撹乱関数（メッセージｍ、乱数ｒ）

$y=\delta_A(d,r)$：乱数成分除去関数（署名ｄ、乱数ｒ）

選挙管理者Ａの署名関数（σ_A、ζ_A）は、乱数による撹乱（ω_A）および乱数成分除去（δ_A）ができるものとする。

【００１１】この署名関数については、例えばＲＳＡ暗号の暗号化関数と復号化関数があり（Ronald Rivest, Adi Shamir, Leonard Adleman: “A method for obtaining digital signatures and public-key cryptosystems”, Communications of the ACM, Vol.21, No.2, pp.120-126(Feb.,1978)）、乱数による撹乱の手法についての詳細は、David Chaum: “Security without identification: Transactionsystems to make big brother obsolete”, Communications of the ACM, Vol.28,No.10, pp.1030-1044(Oct., 1985)に記述されている。

【００１２】以下、投票の手順を示す。

Step 1　投票者V_iは、投票者装置１００を介して投票の準備を次のように行う。

Step 1-1　投票者V_iは、投票内容v_iを乱数発生器１１０よりランダムに選ばれた乱数成分k_iを使用して暗号化器１２０により暗号化し、投票用紙x_i

5

$x_i = \xi(v_i, k_i)$

を作成する。

【0013】Step 1-2　投票者V_iは乱数生成器130を使用してr_iを生成し、撹乱器140を用いて投票文e_i

$e_i = \omega_A(x_i, r_i)$

を作成する。

Step 1-3　投票者V_iは署名作成器150を使用して、e_iの署名s_i

$s_i = \sigma_i(e_i)$

を作成し、e_i、s_iを選挙管理者Aに送信する。

【0014】Step 2　選挙管理者Aは選挙管理装置200を介して承認手続を次のように行う。

Step 2-1　選挙管理者Aは、署名検査器220を使用して、s_iとe_iを検査し、投票者V_iが有権者であることを確認する。もし、そうでなければ、選挙管理者Aは承認を拒否する。

【0015】Step 2-2　選挙管理者Aは、これ以前に投票者V_iが選挙管理者Aによる承認を受けているか否かを検査する。もし、既に承認を受けている場合は、選挙管理者Aは承認を拒否する。

Step 2-3　選挙管理者Aは、e_iを署名作成器230に通して署名d_i

$d_i = \sigma_A(e_i)$

を計算し、e_iに対する承認としてd_iを投票者V_iに送信する。

【0016】Step 3　投票者V_iは投票者装置100を介して、投票用紙とその署名情報を次のように作成する。

Step 3-1　投票者V_iは、d_iとr_iを乱数成分除去器160に入力して投票用紙x_iの署名情報y_i

$y_i = \delta(d_i, r_i)$

を求める。

【0017】Step 3-2　投票者V_iは署名検査器170を使用して、y_iが選挙管理者Aの署名であることを確認する。もし、不合格である場合、投票者V_iはe_i、d_iを示すことにより選挙管理者Aの不正を主張する。

Step 3-3　投票者V_iは、x_i、y_iを集計者Cに集計者装置300および匿名通信路500を介して送信する。

【0018】Step 4　集計者Cは集計者装置300を介して以下のようにして票を収集する。

Step 4-1　集計者Cは集計者装置300および署名検査器310を使用してy_iが投票用紙x_iの署名であることを確認する。もし、合格ならば、集計者Cは投票リスト600に投票用紙x_iとその署名y_iをl、x_i、y_iと番号付けをして掲載する。

【0019】Step 4-2　全ての投票終了後、集計者Cはリストを公表する。このリストは全ての投票者V_iからアクセスすることができるものとする。

6

Step 5　集計者Cは集計者装置300を介して、以下のようにして開票を行う。

Step 5-1　投票者V_iは投票者装置100を介してリストに掲載された投票の数が投票者の数と一致するかどうかを検査する。もし、不合格ならば番号lと乱数r_iを公表して選挙管理者Aの不正を主張する。

【0020】Step 5-2　投票者V_iは自らの投票用紙が掲載されているか否かを検査する。もし、掲載されていなければ、x_i、y_iを公表することにより集計者Cの不正を主張する。

Step 5-3　投票者V_iは、番号lと共に乱数成分k_i、即ちl、k_iを匿名通信路500を介して集計者Cに送信する。

【0021】Step 6　集計者Cは集計者装置300を介して以下のように集計を行う。

Step 6-1　集計者Cは乱数成分k_iを使用して投票用紙x_iを復号化器330にて開票し、投票内容v_iを求め、投票v_iが正しい投票か否かを検査する。

Step 6-2　集計者Cは、投票v_iを集計器340を使用して集計し、その結果を周知するとともに、k_iとv_iをリストに追加する。

【0022】Step 7　投票者V_iは投票者装置100を介して集計者Cの操作が正しいことを確認する。

【0023】

【発明の効果】以上の通りであって、この発明は、投票内容vを暗号化して投票文xを作成するので、選挙管理者Aおよび集計者Cは投票文から投票内容を求めることはできない。そして、投票者V_iは選挙管理者Aに撹乱した投票用紙を署名付きで送信しているので、選挙管理者Aが不正に投票文を混ぜて集計者Cに送信することはできない。これは、選挙管理者Aは不正な投票文に対する署名を保持することができないからである。また、集計者が投票内容を改竄しても、公開された投票内容の一覧表を閲覧することにより投票内容の改竄を検出することができる。即ち、自らの投票が表示されていないときは、暗号化された投票用紙と選挙管理者の署名を公開し、不正を主張すればよい。この際、公開は暗号化されたものを公開するので異議申立時のプライバシーは保証される。この発明は、更に、投票内容を暗号化して送信しているので、投票用紙の収集の際に集計者が途中経過を漏洩して選挙に影響を及ぼすという不正を防止することができる。

【図面の簡単な説明】

【図1】この発明の全体構成を示す図であり、（a）そのブロック図、（b）は投票後の投票内容の一覧を示す図（c）は集計後の投票内容の一覧を示す図である。

【図2】この発明の通信シーケンスを示す図。

【図3】投票者装置のブロック図。

【図4】選挙管理者装置のブロック図。

【図5】集計者装置のブロック図。

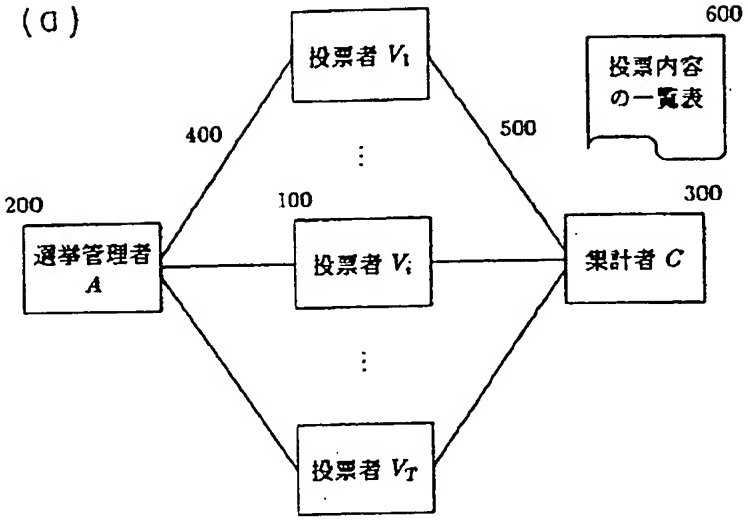
【符号の説明】

100 投票者装置
110 乱数発生器
120 暗号化器
130 乱数発生器
140 撹乱器
150 署名作成器
160 乱数成分除去器
170 署名検査器
200 選挙管理者装置
230 署名作成器
300 集計者装置
310 署名検査器
320 表作成器
340 集計器
600 表

【図1】

図1

(a)



(b)

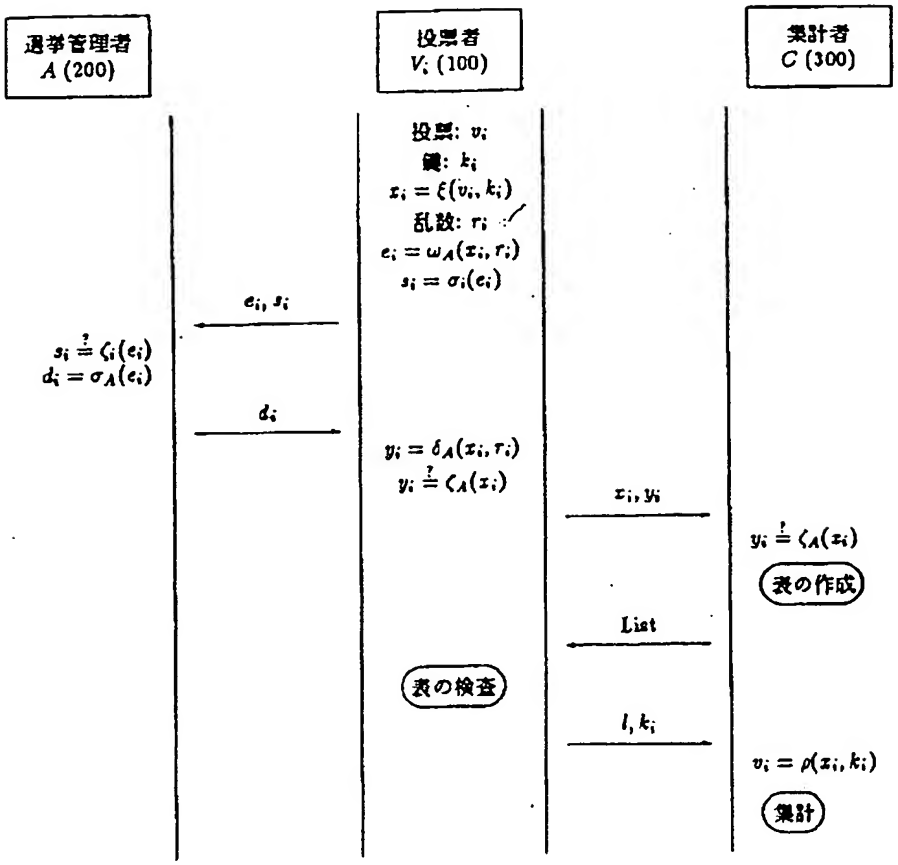
番号	投票内容(付加情報)
1	x_j, y_j
⋮	⋮
l	x_i, y_i
⋮	⋮

(c)

番号	投票内容(付加情報)
1	x_j, y_j, k_j, v_j
⋮	⋮
l	x_i, y_i, k_i, v_i
⋮	⋮

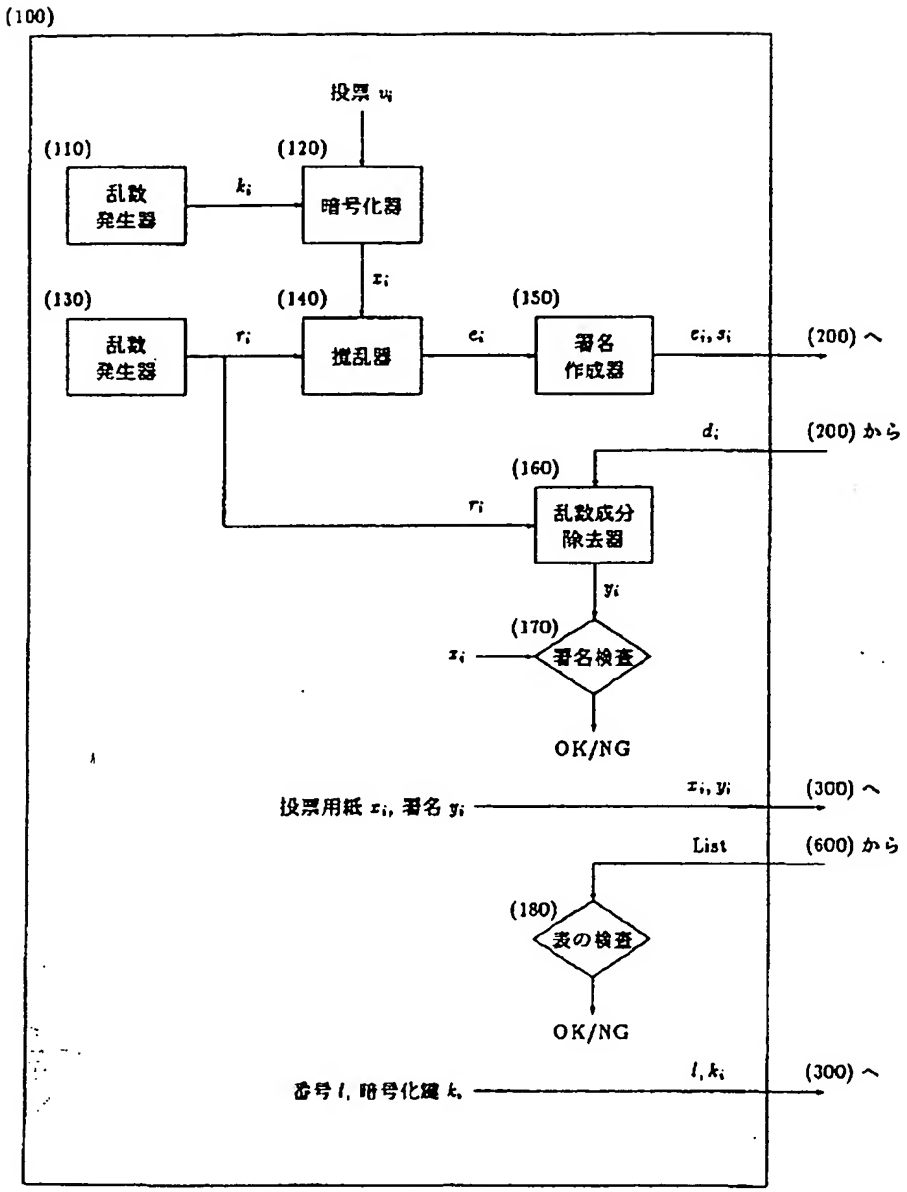
【図2】

図 2


選挙管理者
A (200)
投票者
V_i (100)
集計者
C (300)
投票: v_i
鍵: k_i
$x_i = \xi(v_i, k_i)$
乱数: r_i
$e_i = \omega_A(x_i, r_i)$
$s_i = \sigma_i(e_i)$
e_i, s_i
$s_i \stackrel{?}{=} \zeta_i(e_i)$
$d_i = \sigma_A(e_i)$
d_i
$y_i = \delta_A(x_i, r_i)$
$y_i \stackrel{?}{=} \zeta_A(x_i)$
x_i, y_i
$y_i \stackrel{?}{=} \zeta_A(x_i)$
表の作成
List
表の検査
l, k_i
$v_i = \rho(x_i, k_i)$
集計

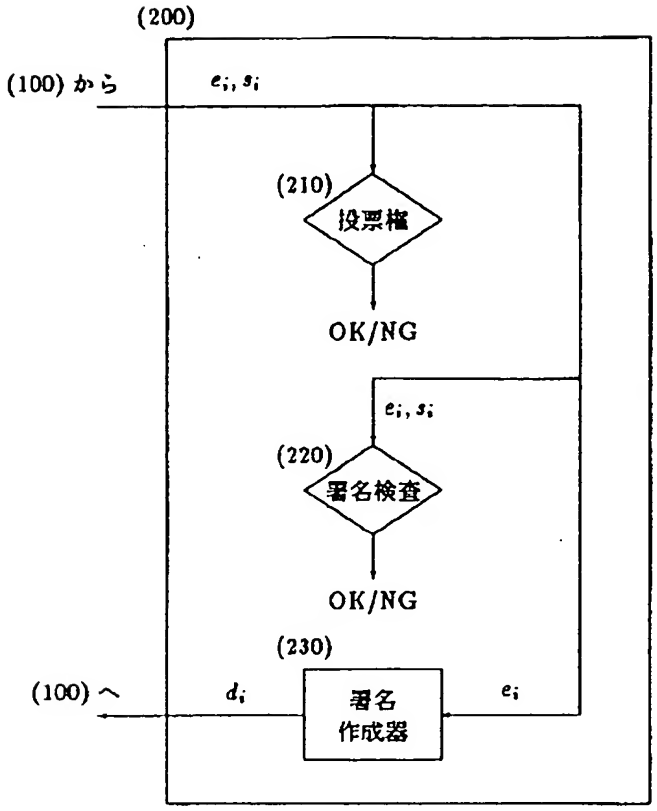
【図3】

図 3


(100)
投票 v_i
(110)
乱数発生器
k_i
(120)
暗号化器
x_i
(130)
乱数発生器
r_i
(140)
撹乱器
e_i
(150)
署名作成器
e_i, s_i
(200) へ
d_i
(200) から
(160)
乱数成分除去器
r_i
y_i
(170)
x_i
署名検査
OK/NG
投票用紙 x_i, 署名 y_i
x_i, y_i
(300) へ
List
(600) から
(180)
表の検査
OK/NG
番号 l, 暗号化鍵 k_i
l, k_i
(300) へ

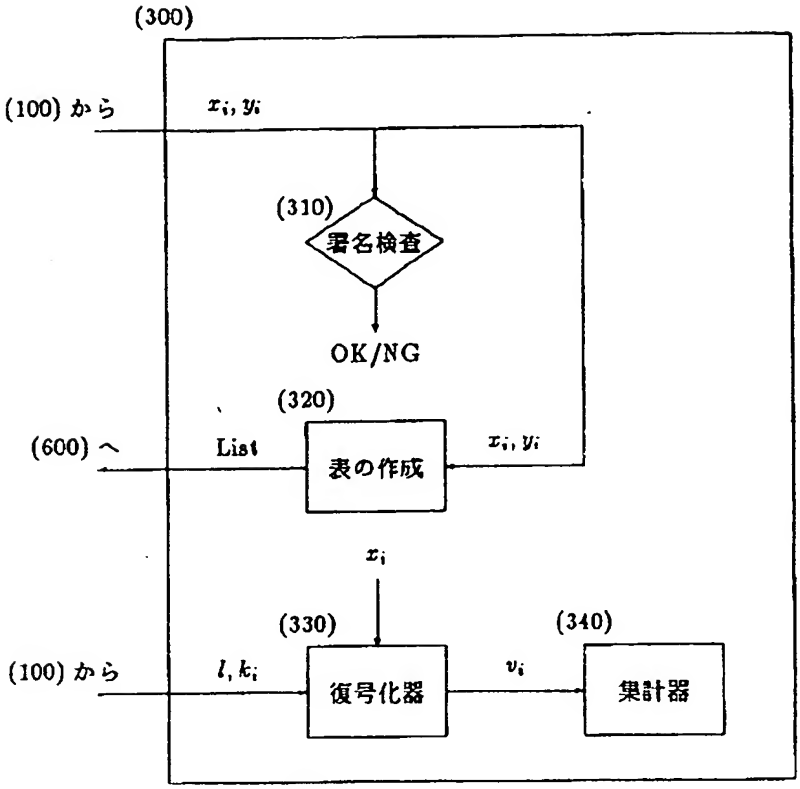
【図4】

図 4


(200)
(100) から
e_i, s_i
(210)
投票権
OK/NG
e_i, s_i
(220)
署名検査
OK/NG
(230)
(100) へ
d_i
署名
作成器
e_i

【図5】

図 5


(300)
(100) から
x_i, y_i
(310)
署名検査
OK/NG
(320)
(600) へ
List
表の作成
x_i, y_i
x_i
(330)
(340)
(100) から
l, k_i
復号化器
v_i
集計器